UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/680,258	10/05/2000	Junichi Kokudo	Q61120	8838

7590	04/28/2004

SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue N.W.
Washington, DC 20037

EXAMINER
ODLAND, DAVID E

ART UNIT	PAPER NUMBER
2662	5

DATE MAILED: 04/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	**Applicant(s)**
	09/680,258	KOKUDO, JUNICHI
Office Action Summary	**Examiner**	**Art Unit**
	David Odland	2662

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2004*.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

    1.☒ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date *3*.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

Response to Amendment

1.   The following is a response to the amendments filed on 03/17/2004.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1-11 are rejected under 35 U.S. C. 103(a) as being unpatentable over applicant's

admitted prior art, hereinafter referred to as APA, and further in view of Lewis (U. S. 6,453,159),

hereinafter referred to as Lewis.

Regarding claim 1, APA teaches a *conventional* authentication method as shown in figure

2 at a wireless LAN system as shown in figure 1, comprising the steps of

-       transmitting an authentication request from a STA to an AP, with which said STA desires

to make association (S 1 of figure 2);

-       *requesting authentication of said authentication request from said AP (authentication*

        request to AP, SI of figure 2)

-       *checking said authentication request at said AP based on a MAC (media access control)*

        address of said STA (S5 of figure 2 and MAC address authentication function on lines 25

        26 of page 1 in the specification);

        - executing encryption authentication at said AP with said STA based on a designated

> *encryption algorithm (executing encryption at S3 of figure 2 based on WEP); and*

- *notifying an authentication completion from said to said AP.*

- *notifying an authentication completion from said AP.*

APA fails to teach an application server and the relationship between the AP and the application server. Lewis teaches an authentication server (key distribution server *76)* as shown in figure 1 that interoperates with APs *54* of figure 1 to add a second encryption layer for additional security that modifies the *conventional steps* above as follows:

- requesting authentication of said authentication request from said AP to an authentication server (the STA authentication request received at the AP is passed to the back bone at step *224* of figure for processing of the second layer by the key distribution server), by converting said authentication request to a protocol adaptable to said authentication server (converting the authentication request to a two layer encryption adapted for the key distribution server *76);*

- checking said authentication request at said authentication server based on a MAC (media access control) address of said STA (checking the authentication request at the key distribution server *76* at step *252* of figure *8* against the system device table *152* of figure the where the authorized device ID or network address, which can be considered a 'MAC address', and inherently the packets includes a MAC address as taught by the APA and IEEE *802.11* taught by Lewis in lines *12-13* of column *6);*

- executing encryption authentication at said AP (executing step *222* of figure *7)* with said STA based on a designated encryption algorithm; and

- notifying an authentication completion from said authentication server to said AP

(authentication completion by the key distribution server at step *262* of figure *8*

appropriately by sending a message to the AP and received and determined by the AP

at step *282* of figure *9)*, after said authentication server received a response of a

completion of said encryption authentication from said AP (after Key distribution

server 76 receives a forwarded message from the AP at step 224 based on step 222 of

figure 7, and see lines 53-54 of column 14).

3.   Regarding claim 2, Lewis further teaches an authentication method at a wireless LAN

system shown in figure 1 in accordance with claim 1, wherein:

- after said encryption authentication is normally completed, a table of said MAC

address in said AP is renewed by an instruction from said authentication server (clear table 126

in the AP taught in lines 36-40 of column 3 is periodically updated by the key distribution server

76 as taught in step 250 of figure 8).

4.   Regarding claim 3, Lewis further teaches an authentication method at a wireless LAN

system in accordance with claim 1, wherein:

- in case that a trouble occurs at said authentication server, said AP itself executes

authentication of said MAC address (the examiner interprets Lewis's method and apparatus as

being consistent with the common philosophies of maximizing network up time, minimizing

down time, and especially avoiding total network outages. With this interpretation should the key

distribution server fail 76, the AP will fall back to conventional techniques for authentication

with the STAB, see line 43 of column 4, have the first layer of protection, and await the recovery

of the key distribution server to recover the second layer protection)

5.   Regarding claim 4, Lewis further teaches an authentication method at a wireless LAN

system in accordance with claim 1, wherein:

-          said encryption algorithm uses a shared key having a predetermined usable period

(shared keys are used at the STA and APS as taught in figure 2, and at the key distribution server

76 as taught in figure 3, and these keys have a period of usage as taught in the access expiration

column of figure 4, and also taught as time limits in line 29 of column 10).

6.   Regarding claim 5, APA teaches an authentication method at a wireless LAN system in

accordance with claim 4, wherein:

-          a MAC address is authenticated by an open system authentication method in line

8 of the specification; and

-          in the open authentication method it is inherent that a key is transported using an

Internet Key Exchange method of Public Key Infrastructure.

APA fails to teach limiting the time for the use of a shared key or reestablishing a shared key

when the predetermined useable period of said shared key expires.

Lewis further teaches:

-          in case that said predetermined usable period of said shared key expired, said

MAC address is authenticated by an open system authentication method (a shared key is limited

in time as cited above in claim 4 in the case that the usable period of said shared key expired the

AP would decide NO at step 222 proceed to step 226 and find the source included in the clear

table and decide yes and pass this to the key distribution server 76 via step 224 in figure 7) ; and

- at said open system authentication method, after association, a period of

communication is limited to a designated short time, and a key is transported in said limited time

by using such an Internet Key Exchange method of Public Key Infrastructure, and said

authentication request is executed again by using said shared key (key distribution server 76 on

receipt of the message from the AP executed at step 224 of figure 7 and would decide yes at step

252 then go to step 254 and decide yes, and then transmit a shared key to the requesting device at

step 256 of figure 8.

It would have been obvious to one of ordinary skill in the art to modify APA's *conventional*

authentication method with the teaching of Lewis and arrive at the claimed invention. One would

have been motivated to make this modification in order to maintain a *conventional* authentication

method and network integrity between the STA and the AP (see lines 49-51 of column 2) while

adding additional security to overcome the potential unauthorized or compromising use of the

network taught by Lewis in lines 58 of column 1 through line 14 of column 2.

7.   Regarding claim 6, APA teaches an authentication apparatus at a wireless LAN system in

figures I and 2, comprising:

- plural STAs I of figure 1; and

- plural APs 2 of figure I

APA fails to teach an application server and the relationship between the AP and the application

server. Lewis teaches an authentication server (key distribution server 76) as shown in figure I

that interoperates with APs 54 of figure 1 to add a second encryption layer for additional security

that modifies the apparatus above as follows

-        plural APs which connect to an authentication server and said plural STAB, and

one of said plural APs receives an authentication request from one of said plural STAB (the STA

authentication request received at the AP is passed to the back bone at step 224 of figure for

processing of the second layer by the key distribution server) and converts said authentication

request from one of said plural STAs to a protocol adaptable to said authentication server

(converting the authentication request to a two layer encryption adapted for the key distribution

server 76), and authenticates said authentication request from one of said plural STAB based on

a designated encryption algorithm (AP executes step 222 of figure 7 and authenticates by

deciding YES); and

-        said authentication server which checks said authentication request from one of said

STAB based on a MAC address of one of said plural STAB by receiving said converted

authentication request (checking the authentication request at the key distribution server 76 at

step 252 of figure 8 against the system device table 152 of figure the where the authorized device

ID, which inherently includes a MAC address taught by the APA and IEEE 802.11 taught by

Lewis in lines 12-13 of column 6, and), and notifies an authentication completion to said AP

(authentication completion by the key distribution server at step 262 of figure 8 appropriately by

sending a message to the AP and received and determined by the AP at step 282 of figure 9),

after said authentication server received a response of a completion of encryption authentication

from said AP (after Key distribution server 76 receives a forwarded message from the AP at step

224 based on step 222 of figure 7, and see lines 53-54 of column 14)

8.   Regarding claim 7, Lewis further teaches an authentication apparatus at a wireless LAN

system shown in figure 1 in accordance with claim 6, wherein:

-       after said encryption authentication is normally completed, a table of said MAC

address in said AP is renewed by an instruction from said authentication server (clear table 126

in the AP taught in lines 36-40 of column 3 is periodically updated by the key distribution server

76 as taught in step 250 of figure 8).

9.   Regarding claim 8, Lewis further teaches an authentication apparatus at a wireless LAN

system in accordance with claim 6, wherein:

-       in case that a trouble occurs at said authentication server, said AP itself executes

authentication of said MAC address (the examiner interprets Lewis's method and apparatus as

being consistent with the common philosophies of maximizing network up time, minimizing

down time, and especially avoiding total network outages. With this interpretation should the key

distribution server fail 76, the AP will fall back to conventional techniques for authentication

with the STAs, see line 43 of column 4, have the first layer of protection, and await the recovery

of the key distribution server to recover the second layer protection)

10.   Regarding claim 9, an authentication apparatus at a wireless LAN system in accordance

with claim 6, wherein:

-        said authentication algorithm is a WEP (wired equivalent privacy) algorithm

stipulated in the IEEE 802.11 (Lewis teaches WEP protocol in an IEEE802.11 standard, see lines

5859 of column 6).

11.   Regarding claim 10, Lewis further teaches an authentication apparatus at a wireless LAN

system in accordance with claim 1, wherein:

-        said encryption algorithm uses a shared key having a predetermined usable period

(shared keys are used at the STA and APS as taught in figure 2, and at the key distribution server

76 as taught in figure 3, and these keys have a period of usage as taught in the access expiration

column of figure 4, and also taught as time limits in line 29 of column 10).

12.   Regarding claim 11, APA teaches an authentication apparatus at a wireless LAN system

in accordance with claim 4, wherein:

-        a MAC address is authenticated by an open system authentication method in line

8 of the specification; and

-        in the open authentication method it is inherent that a key is transported using an

Internet Key Exchange method of Public Key Infrastructure.

It would have been obvious to one of ordinary skill in the art to modify APA's authentication

method with the teaching of Lewis and arrive at the claimed invention. One would have been

motivated to make this modification in order to maintain an existing authentication apparatus and

network integrity between the STA and the AP (see lines 49-51 of column 2) and have no

additional hardware cost associated while adding additional security to overcome the potential

unauthorized or compromising use of the network taught by Lewis in lines 58 of column 1

through line 14 of column 2.

Response to Arguments

4.   Applicant's arguments filed 03/17/2004 have been fully considered but they are not

persuasive.

On page 3-8 regarding the rejections of claims 1-11, the Applicant contends that the

Lewis reference does not teach all of the limitations of the independent claims 1 and 6 because

Lewis teaches of using a network address or ID associated with the mobile terminals and this is

different from the Applicant's invention because the invention uses Media Access Control

(MAC) addresses for performing the authentication check. Specifically, the Applicant argues

that the network address and/or ID in Lewis is a local logical identifier that requires manual input

by a system administrator and can be represented by identifiers such as 'MT1' or 'MT2',

whereas the MAC address of the claimed invention is a globally unique hardware identifier

which is permanently assigned when a device is manufactured and consists of a 48-bit

hexadecimal number. The Examiner respectfully disagrees. Firstly, the Applicant is reminded

that the Examiner must interpret the claims in there broadest sense. Thus, in this case a 'Media

Access Control' address, can be interpreted as merely an address that is used for controlling

which packets have access to a media for transmission. With this interpretation, the 'network

address' and/or 'ID' of the mobile stations in the Lewis reference can clearly be considered

MAC addresses since these identifiers are used to control which packets are transmitted over the

network media and for this reason Lewis does in fact teach the claimed invention. Furthermore,

the Applicant's APA on page 3 lines 15-23 shows that the conventional system uses a MAC

addresses table for authentication but the prior art is limited by having less than 10000 entries in

the table. Therefore, as mentioned in the rejection the APA also teaches this aspect of the

claimed invention. Note, the claim does not recite that the table has more than 10,000 entries

therefore the claim has not been distinguished over the APA and thus the APA does indeed teach

this limitation of the claim. Lastly, although the Applicant, on page 5, has defined the MAC

address of the present invention as being a globally unique hardware identifier which is

permanently assigned when a device is manufactured and consists of a 48-bit hexadecimal

address, neither the specification nor the claim recite any such definition for a 'MAC address'.

In fact, the Applicant's specification describes a very different definition of a MAC address. The

specification defines a MAC address as "...a user name or a calling station ID..." (see page 11

lines 28 and 29 of Applicant's specification). Therefore, the 'network address' and/or 'ID' used

in the Lewis reference clearly meets the Applicant's own definition of the term 'MAC address'

and the rejection is indeed proper.

Conclusion

5.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing
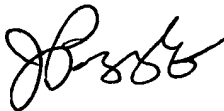
date of this final action.

6.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to David Odland, who can be reached at (703) 305-3231 on Monday

– Friday during the hours of 8am to 5pm.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Hassan Kizou, can be reached at (703) 305-4744. The fax number for the

organization where this application or proceeding is assigned is (703) 872-9306.

        Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist, who can be reached at (703) 305-4750.

deo

April 26, 2004

JOHN PEZZLO
PRIMARY EXAMINER